

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-196085

(43)Date of publication of application : 21.07.1999

(51)Int.Cl.

H04L 9/26

G09C 1/00

H04L 9/32

(21)Application number : 09-370202

(71)Applicant : MICRO TECHNOLOGY KK

(22)Date of filing : 25.12.1997

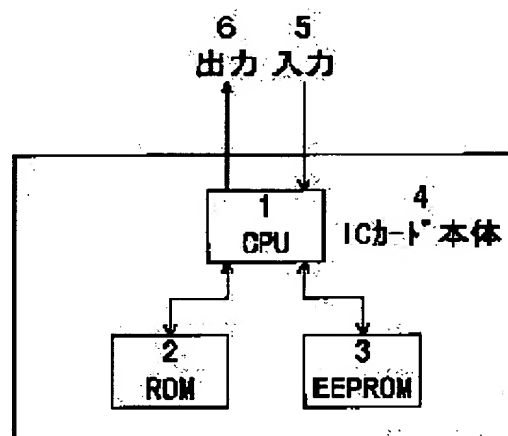
(72)Inventor : SHONO KATSUFUSA

## (54) ENCIPHERMENT RESTORING IC CARD

(57)Abstract:

PROBLEM TO BE SOLVED: To attain the safe management of information in an information communication network by turning a chaos encipherment restoring system into hardware by means of a general-purpose IC card that contains a CPU, a ROM and an EEPROM.

SOLUTION: A CPU 1 is mounted on an IC card main body 4, and an instruction set needed for the exclusive processing is printed to a ROM 2. A database for chaos time series and a cipher key are written into an EEPROM 3. A CPU that has the general-purpose numerical and logical arithmetic capability is also available. The data to be enciphered are stored in a memory of a personal terminal in the form of a file. The blocks divided from a digital file to be enciphered are sent to a register of the CPU 1 from an input part 5. Based on an a command, the CPU 1 retrieves a data base 3 and detects a cipher code to transfer it from an output part 6. Restoration is attained by reversing the enciphering process, even if the base 3 is used in common, however since no time element is needed, thereby, another IC card is available for restoration.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-196085

(43) 公開日 平成11年(1999) 7月21日

(51) Int.Cl.<sup>6</sup>

識別記号

F I

H 0 4 L 9/26

H 0 4 L 9/00

6 5 9

G 0 9 C 1/00

6 3 0

G 0 9 C 1/00

6 3 0 A

H 0 4 L 9/32

H 0 4 L 9/00

6 7 3 E

審査請求 未請求 請求項の数 1 書面 (全 4 頁)

(21) 出願番号

特願平9-370202

(22) 出願日

平成 9 年 (1997) 12 月 25 日

(71) 出願人 591233810

マイクロテクノロジー株式会社

東京都文京区大塚 6 丁目 7 番 4 - 302 号

(72) 発明者 庄野 克房

神奈川県横浜市旭区白根 5 丁目 45 番 12 号

(54) 【発明の名称】 暗号化復元用 I C カード

(57) 【要約】

【目的】 コンピュータと通信を主要な構成要素とする情報通信ネットワークにおいて、個人の情報の安全管理を容易にするデジタルデータ暗号化復元装置を提供する。

【構成】 中央演算装置 (C P U) を搭載した I C カードにおいて、カオス暗号専用の処理を行う命令セットを R O M に書き込み、データ量を縮小と検索の高速化をはかるために時間要素を残してテーブル化したカオスのタイムシリーズと暗号鍵を E E P R O M に書き込んでおく。

**THIS PAGE BLANK (USPTO)**

## 【特許請求の範囲】

【請求項1】 中央演算装置 (central processing unit: CPUと略す) が検索機能を持ち、記憶装置 (メモリ) に命令セットとカオスのタイムシリーズのデータベースを持つことを特長とする暗号化復元用 IC カード。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 コンピュータと通信を主要な構成要素とする今日の情報通信ネットワークにおいては、いろいろなレベルで情報の安全管理が必要とされる。安全管理の手段として暗号が用いられる。

【0002】 ネットワークの中のサーバーに暗号化復元機能をもたせるのは、集团的安全管理の手法である。

【0003】 個人端末において、ユーザ各人が自己責任において情報の安全管理を行う場合もある。本案は個人の情報管理のための暗号化復元用 IC カードに関する。

## 【0004】

【従来の技術】 カオスの観測可能なタイムシリーズを非線形に量子化し、縮退した量子に分割したデジタルブロックを対応させて暗号鍵とし、タイムシリーズ上を検索して暗号化復元を行う、カオスの秩序を利用した暗号化復元の手法は既に知られている。

【0005】 カオスの発生は電子回路的に行っても、非線形写像関数を精度が保証された計算手法によって求めたものでも、いづれでもよい。

【0006】 非線形量子化を非線形 ADC (アナログデジタル変換器) を用いて回路的に行っても、いったんタイムシリーズを計算機内のメモリに記憶したあと非線形区分を与えて量子化してもよい。

【0007】 カオス暗号の特長は、同じ暗号化すべきデジタルファイルを繰り返し暗号化したとき、同じ暗号鍵を用いても、常に異なる暗号コードが生成されることである。

## 【0008】

【発明が解決しようとする課題】 カオス暗号は専らソフトウェアとして提供されてきた。情報の安全管理がソフトウェアの管理に置き換えられている。ソフトウェアは誰にでも容易にコピーがとれる。ダウンロードした使用状態からでもコピーがとられる危険がある。これらの危険を回避するために、IC カードのハードウェアとして暗号化復元システムを提供するのが本案である。

## 【0009】

【課題を解決するための手段】 IC カードには、規模が小さくても CPU が搭載されているものがある。専用の処理をするための命令セットは ROM に焼き付けられている。カオスタイムシリーズのデータベースと暗号鍵が EEPROM に書き込まれる。

【0010】 非線形量子化により生成される縮退した量子の量子サイズをそろえたタイムシリーズをそのまま E

EPROM に書き込むと、当然のことながら、膨大なデータ量となる。

【0011】 暗号化にあたって検索を行うときには、たとえば 8 ビット 256 量子に量子化したタイムシリーズでは、検索して発見したデータ  $y(t)$  に対し標準的には 4 ステップ過去の値  $y(t-4)$  を暗号コードとする。時間要素を残してテーブル化することにより検索を高速に実行でき、タイムシリーズのデータを圧縮することができる。また、検索に工夫をすることにより、時間要素を取り除いたテーブルを検索するようにしてもよい。例えば 8 ビットに量子化した場合、16 行 16 列のテーブルとなる。行の並べ方が暗号鍵となる。

【0012】 カオスのタイムシリーズにはフラクタル性が保存されている。タイムシリーズのある範囲のみのデータを検索用のデータベースとして EEPROM に書き込んでおくことで、繰り返し暗号化したときに異なる暗号コードが生成されるというカオス暗号の特長が失われることはない。

## 【0013】

【作用】 IC カードの構成の 1 例を図 1 に示す。1 は検索機能をもつ CPU である。汎用の数値演算及び論理演算能力をもつ CPU でよい。必要な命令コードのセットは ROM 2 に格納されている。EEPROM 3 に非線形量子化したカオスのタイムシリーズがデータベースのテーブルとして記憶される。同時に暗号鍵もセットされている。

【0014】 暗号化すべきデータはファイルとして個人用端末のメモリ内に保管されている。暗号化すべきデジタルファイルの分割されたブロックが、入力 5 から CPU のレジスタに送られ、命令に従って CPU はデータベース 3 を検索し暗号コードを発見し、出力 6 から転送する。これが暗号化の過程である。

【0015】 復元は暗号化の逆過程である。データベース 3 を共通にしても実行できるが、暗号化のデータベース 3 には時間要素を残したテーブルを用い、暗号コードにカオスの予測不可能な特長を残すようにし、復元用のデータベース 3 には時間要素は必要としない。暗号化用と復元用に別々の IC カード 4 を用いてもよい。

## 【0016】

【実施例】 図 1 の実施例にもとづいて、詳しい具体例を示す。暗号化すべきデジタルファイルを 4 ビットブロックに分割する場合を説明する。4 ビットブロックコードの 1 つ、例えば、(0100) が CPU に転送されるものとする。

【0017】 データベース 3 には 16 種類の縮退した量子をもつ 8 ビットのタイムシリーズが時間要素を残してインストールされている。暗号鍵の配列にしたがって入力コード (0100) に相当するテーブルの行列が検索され、命令 2 の指示に従って 8 ビット暗号コードが 1 つ選択される。そのコードが (10100101) という

**THIS PAGE BLANK (USPTO)**

8ビットコードであったとすると、入力コード(0100)が8ビット(10100101)という暗号コードに変換されたことになる。出力6から暗号コード(10100101)が転送される。この過程を繰り返して、暗号化すべきデジタルファイルのすべての情報が暗号ファイルに変換され、転送される。

【0018】4ビット入力コード16種類を16種類の縮退した量子に対応させる、その組み合わせが暗号鍵である。暗号鍵の発行できる種類は、この場合、 $16! = 2.09 \times 10^{13}$ 通りもある。鍵の発行は距離計算をして、十分離れた距離にある鍵をコンピュータが自動発行・管理する。

【0019】同じICカードで復元も行う場合には、暗号コード8ビットを入力5から転送してくることによる。上位4ビットと下位4ビットに分割して送ればよい。暗号コードをタイムシリーズのデータベース上で検索し、対応する縮退した量子の4ビットコードを求め、出力6より転送する。

【0020】この実施例のように4ビットコードが8ビットコードに暗号化され、8ビット暗号コードが4ビットコードに復元されるときには、CPUは8ビットデータバスをもつ、例えば、Z-80のような演算装置でよい。

【0021】暗号化すべきデジタルファイルが文書やデータなどの場合、分割されるデジタルブロックの長さは4ビットか8ビットが適当である。一方、音声のように、周波数分解された音声信号がAD変換され音質を保証するのに上位5ビットを暗号化、転送、復元する場合には、5ビットブロックが適当である。音声の実時間での暗号化復元を実行する場合には、単位ブロックを5ビットにしたシステムの設計をする方が合理的である。

【0022】暗号鍵の発行にあたって基本操作(シフト、回転、反転、置換など)を加えて、ICカードを階層的に構造化することもできる。

【0023】カオスの秩序を利用して、階層的に構造化した暗号化復元システムの特長は、Aという鍵で暗号化したあと、誤ってBという鍵で復号したとき、当然復号

に失敗するが、誤って復号化したファイルから復帰する手法がある。誤ったファイルをいったんBで暗号化する。そのあとAで復号すれば、原文にたどり着くことができる。秩序も構造化されているからである。

【0024】

【発明の効果】暗号化復元処理をソフトウェアで実行するのも便利な手法ではあるが、誰にでも容易にコピーがとれるという点では安全性は損なわれる。ハードウェアの管理はソフトウェアに比べると容易である。本案は、CPU、ROM及びEEPROMを搭載した汎用性のあるICカードを用いてカオス暗号化復元システムをハードウェア化した。

【0025】CPU、ROM、EEPROMを搭載したICカードは、CPUを共通にしてROMの命令コードセットやEEPROMのカオスのデータベースに固有のものを書き込むことにより専用化できる。共通のハードウェア資源を活用して、個別の専用化に対応できる手法である。

【0026】暗号化用ICカードと復元用ICカードを共通の1枚のカードに統合することもできる。2つに分ける方が処理速度は向上し、音声や画像の実時間処理に都合がよい。

【0027】ICカードに固有の鍵が与えられるのが本案の原則であるが、鍵の構成に基本操作を加えることにより、複数のICカードに関し暗号化復元システムを階層的に構成することもできる。以上詳しく説明してきたように、本案は情報通信ネットワークにおいて安全な情報管理を実現する新規の手法を提案している。

【図面の簡単な説明】

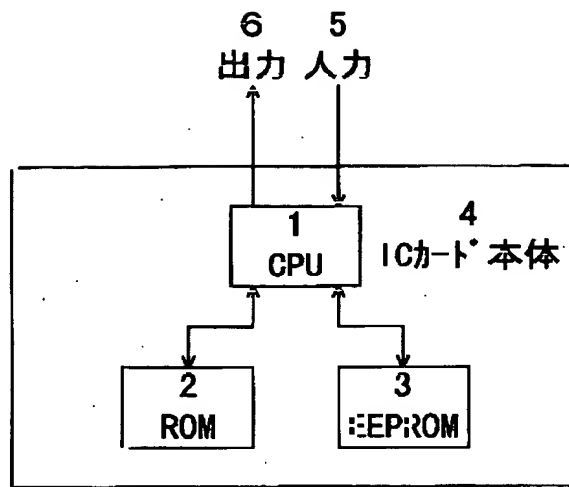
【図1】暗号化復元用ICカードの構成図である。

【符号の説明】

- 1 CPU
- 2 ROM
- 3 EEPROM
- 4 ICカード本体
- 5 入力
- 6 出力

THIS PAGE BLANK (USPTO)

【図1】



**THIS PAGE BLANK (HSPTO)**